Date	Event
8-Oct-03	NSA-FBI-CIA conference at NSA to discuss PSP operations and customer needs
15-Oct-03	**20th Presidential Authorization signed**
[redacted]	[redacted]
1-Dec-03	NSA IG announces a review of NSA PSP operations
8-Dec-03	NSA IG asks VP Counsel for access to PSP legal opinions and is told that a request should come from General Hayden
9-Dec-03	**21st Presidential Authorization signed**
9-Dec-03	IG memo asks General Hayden to ask VP Counsel's permission for NSA IG and GC to obtain copies of, or view, PSP legal justification
[redacted]	[redacted]
2004	
6-Jan-04	NSA briefing to DoJ Mr. Philbin, Mr. Goldsmith for Mr. Goldsmith's orientation to the PSP and other NSA Signals Intelligence efforts against terrorism
8-Jan-04	NSA and FBI [redacted] meet to discuss the PSP and recent changes at NSA
14-Jan-04	**22nd Presidential Authorization signed**
[redacted]	[redacted]
9-Mar-04	General Hayden briefs Director of Central Intelligence (DCI) on value of the PSP
10-Mar-04	General Hayden briefs White House Counsel and Chief of Staff, Deputy DCI, Deputy AG, and FBI Director on value of the PSP
10-Mar-04	General Hayden briefs Speaker of the House, Senate Majority and Minority leaders, House Minority Leader, Chairman and Ranking Member, HPSCI, and Chair and Vice Chair, SSCI
10-Mar-04	General Hayden briefs Secretary of Defense, DoD Principal Deputy GC
11-Mar-04	**23rd Presidential Authorization signed**
11-Mar-04	NSA IG and Acting GC discuss new Authorization signed by President's Counsel rather than the AG
11-Mar-04	NSA briefs House Majority Leader
[redacted]	[redacted]
12-Mar-04	General Hayden briefs House Majority Leader
19-Mar-04	**Revision to 23rd Presidential Authorization signed**
[redacted]	General Hayden sends letter to Assistant AG, Office of Legal Counsel (OLC) [redacted]

Date	Event
	[redacted]
2-Apr-04	**2nd Revision to 23rd Presidential Authorization signed**
4-Apr-04	General Hayden briefs DoD Principal Deputy GC
5-May-04	**24th Presidential Authorization signed**
[redacted]	[redacted]
20-May-04	NSA briefs the Minority Leader of the Senate
[redacted]	[redacted]
23-Jun-04	**25th Presidential Authorization signed**
[redacted]	[redacted]
14-Jul-04	Initial PR/TT Order approved by FISC
9-Aug-04	**26th Presidential Authorization signed**
[redacted]	[redacted]
23-Aug-04	General Hayden briefs National Security Advisor and Homeland Security Advisor
[redacted]	
17-Sep-04	**27th Presidential Authorization signed**
[redacted]	[redacted]
23-Sep-04	Presidential "further direction" of 9 August 2004 expires
23-Sep-04	NSA briefs Chair, HPSCI
[redacted]	
17-Nov-04	**28th Presidential Authorization signed**
[redacted]	[redacted]
2005	
5-Jan-05	NSA briefs National Security Advisor and White House Counsel
[redacted]	[redacted]
11-Jan-05	**29th Presidential Authorization signed**

Date	Event
[redacted]	[redacted]
3-Feb-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
25-Feb-05	General Hayden briefs White House Counsel and Counsel to Deputy AG
1-Mar-05	**30th Presidential Authorization signed**
2-Mar-05	NSA briefs Senate Minority Leader
[redacted]	[redacted]
19-Apr-05	**31st Presidential Authorization signed**
[redacted]	[redacted]
22-Apr-05	General Hayden briefs Director of National Intelligence (DNI)
23-May-05	Two-level PSP clearance structure discontinued
1-Jun-05	Discussions to seek FISC orders to authorize content collection begin with DoJ OLC
14-Jun-05	**32nd Presidential Authorization signed**
[redacted]	[redacted]
26-Jul-05	**33rd Presidential Authorization signed**
[redacted]	[redacted]
3-Aug-05	Principal Deputy DNI Hayden briefs new NSA/CSS Director General Alexander on the PSP
10-Sep-05	**34th Presidential Authorization signed**
14-Sep-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
26-Oct-05	**35th Presidential Authorization signed**
[redacted]	[redacted]
13-Dec-05	**36th Presidential Authorization signed**
16-Dec-05	New York Times says that President secretly authorized NSA eavesdropping on Americans
[redacted]	[redacted]
20-Dec-05	DoD IG receives letter, signed by 39 Congressmen, requesting a review of the PSP. DoD IG faxes the letter to the NSA IG on 10 Jan 06
21-Dec-05	NSA briefs DNI

Date	Event
2006	
3-Jan-06	NSA IG and DoD IG discuss letter from 39 Congressmen requesting DoD IG review of the PSP
9-Jan-06	NSA briefs nine FISC judges and three FISC legal advisors
11-Jan-06	NSA briefs Speaker of the House, Senate Majority Leader, Chair of HPSCI, Chair and Vice Chair, SSCI
20-Jan-06	NSA briefs Senate Minority Leader, House Minority Leader, Chair SSCI, and Ranking Member HPSCI
[redacted]	[redacted]
27-Jan-06	**37th Presidential Authorization signed**
31-Jan-06	NSA briefs FISC Judge Scullin
[redacted]	[redacted]
11-Feb-06	NSA briefs Chair SSCI
16-Feb-06	NSA briefs Speaker of the House and Chair, HPSCI
28-Feb-06	NSA briefs Chair and Ranking Member, House Appropriations Subcommittee on Defense
[redacted]	
3-Mar-06	NSA briefs Vice Chair, SSCI
9-Mar-06	NSA briefs Chair and Vice Chair, SSCI, and Members of SSCI Terrorist Surveillance Program (TSP) Subcommittee (Roberts, Rockefeller, Hatch, DeWine, Feinstein, Levin, Bond) with SSCI Minority and Majority Staff Directors, Senior Director for Legislative Affairs, National Security Counsel, VP, AG, White House Counsel, and VP Chief of Staff
10-Mar-06	NSA briefs Mr. Bond, Member, SSCI TSP Subcommittee
13-Mar-06	NSA briefs Chair, SSCI TSP Subcommittee, Members SSCI TSP Subcommittee (Roberts, Feinstein, and Hatch), SSCI Majority and Minority Staff Directors, and SSCI Counsel at NSA
14-Mar-06	NSA briefs Mr. DeWine, Member, SSCI TSP Subcommittee at NSA
21-Mar-06	**38th Presidential Authorization signed**
21-Mar-06	NSA briefs FISC Judge Bates
[redacted]	[redacted]
27-Mar-06	NSA briefs Mr. Levin, Member, SSCI TSP Subcommittee and Minority Staff Director at NSA
29-Mar-06	NSA briefs Chairman and Ranking Member HPSCI TSP Subcommittee, TSP Subcommittee Members (Hoekstra, Harman, McHugh, Rogers, Thornberry, Wilson, Davis, Holt, Cramer, Eshoo, and Boswell), Majority General Counsel, Staff Member, and Minority General Counsel

Date	Event
7-Apr-06	NSA briefs Chairman of the HPSCI TSP Subcommittee, HPSCI TSP Subcommittee Members (Hoekstra, McHugh, Rogers, Thornberry, Wilson, and Holt), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	[redacted]
28-Apr-06	NSA briefs Ranking Member, HPSCI TSP Subcommittee, Members of HPSCI TSP Subcommittee (Harman, Wilson, and Eshoo), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	
11-May-06	NSA briefs Chair and Ranking Member House Appropriations Committee Defense Subcommittee
16-May-06	**39th Presidential Authorization signed**
17-May-06	Chair SSCI, Members, SSCI (Roberts, Hagel, Mikulski, Snowe, DeWine, Bayh, Chambliss, Lott, Bond, Levin, Feingold, Feinstein, Wyden, Warner), SSCI Staff Member, SSCI Majority Staff Director, and SSCI Counsel
17-May-06	HPSCI Chair, HPSCI Members (Hoekstra, Harman, Wilson, Eshoo, Rogers, Thornberry, Holt, Boswell, Cramer, LaHood, Everett, Gallegly, Davis, Tiahrt, Reyes, Ruppersberger, and Tierney), Majority General Counsel, Staff Director, and Minority General Counsel
[redacted]	[redacted]
24-May-06	First Business Records Order approved by the FISC
5-Jun-06	NSA briefs Ms. Feingold, SSCI Member at NSA
7-Jun-06	NSA briefs Ranking Member, Senate Defense Appropriations Subcommittee, and SSCI Staff Director
7-Jun-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
9-Jun-06	NSA briefs Chair, SSCI, SSCI Members (Mikulski, Wyden, and Hagel), SSCI Minority Staff Director, SSCI Counsel, and SSCI Staff Director
15-Jun-06	NSA briefs Chair, SSCI and SSCI Members (Roberts, Mikulski, Feingold, Bayh, Snowe, Hatch, Lott, and Bond), and Minority Staff Director
26-Jun-06	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and House Minority Leader
30-Jun-06	NSA briefs Mr. Bayh, SSCI Member at NSA
6-Jul-06	**40th Presidential Authorization signed**
[redacted]	[redacted]
10-Jul-06	NSA briefs Ms. Snowe, SSCI Member and SSCI Counsel at NSA
18-Jul-06	NSA briefs Mr. Chambliss, SSCI Member at NSA
[redacted]	
6-Sep-06	**41st Presidential Authorization signed**
[redacted]	[redacted]

Date	Event
[redacted]	[redacted]
24-Oct-06	**42nd Presidential Authorization signed**
[redacted]	[redacted]
20-Nov-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
8-Dec-06	**43rd and final Presidential Authorization signed**
[redacted]	[redacted]

2007

10-Jan-07	Content orders approved by the FISC
17-Jan-07	AG letter to Congress: Presidential program brought under the FISC
1-Feb-07	NSA briefs President's Privacy and Civil Liberties Oversight Board
1-Feb-07	Presidential Authorization expires

~~(TS//STLW//SI//OC/NF)~~

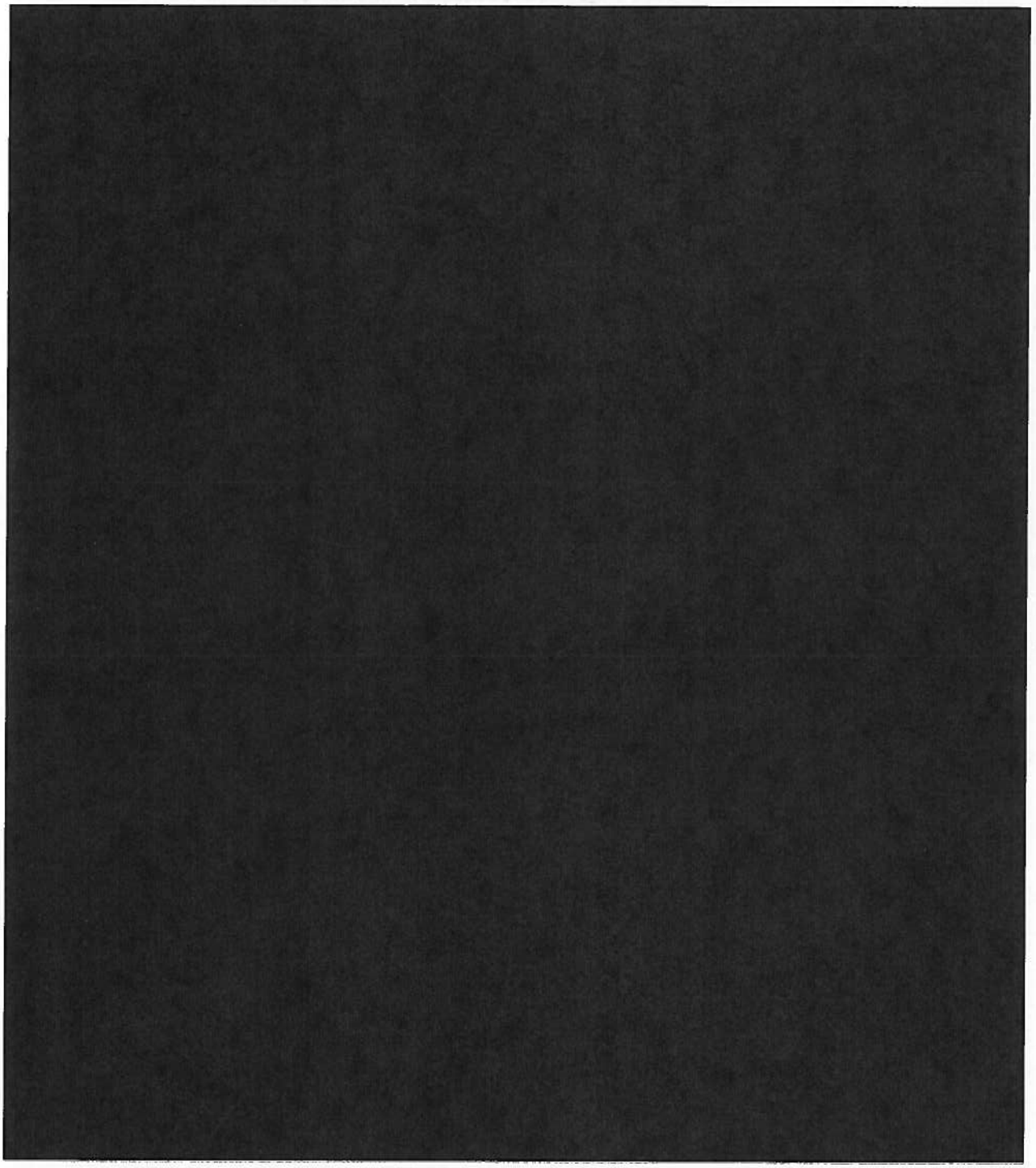
This page intentionally left blank.

APPENDIX D

(U) Cumulative Number of Clearances for the President's Surveillance Program

This page intentionally left blank.

(U) Cumulative Number of Clearances for the President's Surveillance Program[4]



This page intentionally left blank.

APPENDIX E

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

This page intentionally left blank.

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

~~(TS//SI//NF)~~ This appendix lists and describes OIG investigation and review reports of activity conducted under the PSP, also referred to as the STELLARWIND Program, and related activities such as the Pen Register Trap and Trace (PR/TT) Order and the Business Records Order. These reports are limited to activity conducted between 4 October 2001 and 17 January 2007.

(U) OIG Investigations

[redacted]

(U) Report of Investigation of Two Violations

~~(S//NF)~~ On [redacted] the OIG issued a report on what it believed to be the first two violations of Authorization, both of which were unintentional.

~~(TS//STLW//SI//OC/NF)~~ The first incident occurred on [redacted] An NSA analyst misguidedly used PSP authority to collect communications between [redacted] These communications were foreign within the meaning of the Authorization, but they were not terrorist related. [redacted]

~~(TS//STLW//SI//OC/NF)~~ The second incident occurred on [redacted] when NSA inappropriately performed contact chaining on [redacted] This query was requested by an FBI official during the investigation of [redacted]

~~(S//NF)~~ NSA OIG found that in neither incident had NSA personnel acted with intent to disregard their authority.

Both incidents occurred, at least in part, because early in the Program the terms of the Authorization were so closely held that few, if any, operational personnel working under the Authority were permitted to see the Authorization or its operative provisions. It was unreasonable to hold persons accountable for violating an order that they had not seen, when the order was too complex to be easily committed to memory. Accordingly, the OIG did not recommend disciplinary action, but did recommend that the NSA Director issue formal written delegations of authority to the Signals Intelligence Director and specified subordinates so that personnel working the Program would know the precise terms of the Authorization. Management concurred with the recommendations and made appropriate notifications.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

[redacted] ~~(TS//SI//NF)~~ ***Violations of Court Orders in*** [redacted]

Foreign Intelligence Surveillance Court

~~(TS//STLW//SI//OC/NF~~ On 14 July 2004 [redacted] The Order permitted NSA to collect Internet metadata under the pen register/trap-and-trace provisions of the FISA (§§ 1841-1846). The authority to collect Internet metadata under the Order [redacted] Material acquired under the Order continued to be protected in PSP channels.

~~(TS//STLW//SI//OC/NF)~~ On [redacted] NSA OIG issued a report on an investigation of a management breakdown that had resulted in unintentional filtering violations of the FISC Order. The Order permitted NSA to collect Internet metadata from communications involving [redacted] The violations occurred because NSA [redacted] However, no violations resulted from the collection of domestic communications. An NSA collection manager discovered the violations on [redacted]. The following day, the questionable collection was stopped and reported to the OIG and the OGC. With the exception of [redacted] the OIG

found no reason to believe that any violations resulted in the collection of U.S. person information. The OIG reserved judgment on [redacted] The OIG evaluation of responsibility for the incident led directly to the replacement of the Program Manager and to changes in Program management, leadership, and chain of command.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

(~~TS//SI//NF~~) Supplemental Report on Violations of Court Orders in [redacted]

~~(TS//STLW//SI//OC/NF)~~ A follow-up investigation of the questionable [redacted] revealed no additional violations. On [redacted], the NSA OIG issued a report detailing its examination of [redacted] that the OIG suspected might not have originated or terminated outside the United States. [redacted] All but [redacted] messages could have been associated with a foreign sender or recipient. [redacted] None of the [redacted] messages had been intentionally collected, none had been analyzed, and none had been reported outside NSA.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

(U) OIG Reviews

14 May 2004 ***(U) Need for Documentation and Development of Key Processes (ST-04-0024)***

~~(TS//SI//NF)~~ This OIG report concluded that a continuing deficiency in clear, written procedures governing the collection, processing, and dissemination of PSP material created undue risk of unintentional violations of the Authorization. The report noted that Program officials had

made progress in addressing some of these deficiencies, but found that processes had not been fully documented in the form of management directives, administrative policies, or operating manuals. The NSA OIG recommended that Program officials formally adopt rigorous, written operating procedures for the following key processes:

- Approvals for content collection by the appropriate named officials
- Reporting of violations of the Authority, similar to procedures for documenting violations of Legal Compliance and Minimization Procedures[5]
- Evaluation of dual FISA and PSP content collection
- Systematic identification and evaluation of telephone numbers and Internet identifiers for detasking.[6]

(U//~~FOUO~~) Corrective action was taken in response to the four recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 06 and HPSCI on 2 January 2008.

13 Sep 2004 ***~~(S//NF)~~ Need for Increased Attention to Security-Related Aspects of the STELLARWIND Program (ST-04-0025)***

(U//~~FOUO~~) This OIG report disclosed weaknesses in Program security. The Program was particularly vulnerable to exposure because it involved numerous organizations inside and outside NSA.

(U//~~FOUO~~) While the Program Manager placed a strong emphasis on personnel security, he did not take a proactive and strategic approach to physical and operational security. In particular, better use of the Program Security Officer would have helped to improve special security practices for handling Program material and strengthen operations security (OPSEC).

(U//~~FOUO~~) The Program Manager and the Associate Director for Security and Counterintelligence concurred with the findings and implemented corrective measures. In particular,

---

[5](U) U.S. Signals Intelligence Directive 18 or "USSID SP0018" (as of 27 July 2003).
[6](~~TS//SI//NF~~) [redacted]

the Staff Security Officer was freed from other responsibilities and took a more active and effective role in Program security. Management did not conduct a formal OPSEC survey as recommended; however, steps taken by management to implement OPSEC practices met the intent of the original recommendation.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

21 Nov 2005 ***~~(TS//SI//NF)~~ Review of the Tasking Process for STELLARWIND U.S. Content Collection (ST-04-0026)***

~~(TS//STLW//SI//OC/NF)~~ This report identified material weaknesses in the tasking and detasking process under the PSP. The process to task and detask telephone numbers for content collection under the Program was inherently fragile because it was based on e-mail exchanges and was not automated or monitored.

~~(TS//STLW//SI//OC/NF)~~ The OIG examined [redacted] telephone numbers and Internet identifiers approved for content collection on the date in November 2004 when the audit began and identified the following types of errors:

- [redacted] involved under-collection; identifiers were not put on collection quickly enough or were not put on collection until the OIG discovered the errors.
- [redacted] involved unauthorized collection caused by a typographical error.
- [redacted] involved over-collection; they were not removed from collection quickly enough.
- [redacted] record-keeping errors in the Program's tracking database

~~(TS//STLW//SI//OC/NF)~~ In the [redacted] of unauthorized collection caused by a typographical error, NSA personnel did not review the collected information before destroying it, nor did NSA issue any report based on, or otherwise disseminate, any information from the [redacted] of untimely detasking. However, without a robust and reliable collection and tracking process, NSA increased its risk of unintentionally violating the Authorization. NSA also increased the risk of missing

valuable foreign intelligence by failing to task telephone numbers and Internet identifiers in a timely manner.

(U//~~FOUO~~) NSA OIG recommended that all errors be swiftly resolved, that specific procedures be adopted to prevent recurrences, and that identifiers tasked for collection be promptly reconciled with identifiers approved for tasking, and repeated every 90 days. Management implemented the recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

31 May 2006 ~~(TS//SI//NF)~~ ***Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027)***

~~(TS//STLW//SI//OC/NF)~~ This report determined that, based on a statistical sample, Program officials were adhering to the terms of the Authorization and the Director's delegation thereunder; that tasking was appropriately approved and duly recorded under the Authorization; and that tasking was justified as linked to al-Qa'ida or affiliates of al-Qa'ida. The report recommended improvements in record-keeping practices.

~~(S//NF)~~ Due to a lack of sufficient and reliable data, the NSA OIG could not reach a conclusion on the tasking approval process for two PSP-related collection programs. The OIG recommended that management responsible for the affected programs, design and implement a tasking and tracking process to allow managers to audit, assess timeliness, and validate the sequencing of tasking activities. Management agreed to install automated tracking of tasking and detasking.

~~(TS//SI//NF)~~ Although the collection architecture was designed to produce one-end-foreign communications, inadvertent collection of domestic communications occurred and was addressed. The OIG recommended changes in management reporting to improve the tracking and resolution of inadvertent collection issues.

(U//~~FOUO~~) Corrective action has been completed for one of the two recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

11 Jul 2006 ~~(TS//SI//NF)~~ ***Supplemental Report to Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027.01)***

~~(TS//STLW//SI//OC/NF)~~ After issuing the original report, the NSA OIG conducted further research to determine whether Program officials were approving content tasking requests based solely on metadata analysis. Using the statistical sample in the original audit, the OIG found no instances of metadata analysis as the sole justification for content tasking. In all cases tested, there was corroborating evidence to support the tasking decision.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

5 Sep 2006 ~~(TS//SI//NF)~~ ***Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records (ST-06-0018)***

~~(TS//STLW//SI//OC/NF)~~ On 24 May 2006, the telephony metadata portion of the PSP was transferred to FISC Order BR-06-05, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [Telecommunications Providers] *Relating to* [redacted] The Order authorized NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data regarding [redacted]

~~(TS//SI//NF)~~ On 10 July 2006, in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*, the NSA OIG issued "a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." This report was issued with the Office of the General Counsel's concurrence as mandated by the Order.

~~(TS//SI//NF)~~ The "*Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance*

Court Order: Telephony Business Records (ST-06-0018)," 5 September 2006, provided the details of the findings of the 10 July memorandum and made formal recommendations to management.

~~(TS//SI//NF)~~ Management controls governing the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order were adequate and in several aspects exceeded the terms of the Order. However, due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, the NSA OIG recommended three additional controls regarding collection procedures, reconciliation of audit logs, and segregation of duties.

~~(TS//SI//NF)~~ Collection Procedures

~~(TS//SI//NF)~~ During an OIG review of collection procedures, Program management discovered that NSA was obtaining [redacted] data that might not have been in keeping with the Order: [redacted] OGC advised that [redacted] data should have been suppressed from the incoming data flow. Immediately, management blocked the data from analysts' view. Further, working with the providers, Program management completed suppression of the suspect data on 11 October 2006 and agreed to implement additional procedures to prevent the collection of unauthorized data.

~~(TS//SI//NF)~~ Reconciliation of Audit Logs

~~(TS//SI//NF)~~ Management controls were not in place to verify that telephone numbers approved for querying were the only numbers queried. Although audit logs documented the queries of the archived metadata, the logs were not in a usable format, and Program management did not routinely use them to audit telephone numbers queried. Management concurred with the recommendation to conduct periodic reconciliations; however, action was contingent on the approval of a Program management request for two additional computer Programmers.

[redacted]

~~(C//NF)~~ Lack of Segregation of Duties

~~(C//NF)~~ The seven individuals with the authority to approve queries also had the ability to conduct queries under the Order. Standard internal control practices require that key duties and responsibilities be divided among different people to reduce the risk of error and fraud. Although Program management concurred with the finding, it could not implement the recommendation due to staffing and operational needs. As an alternative, Program management agreed to develop a process to monitor independently the queries of the seven individuals. This action plan was contingent on the development of usable audit logs recommended above.

(U//~~FOUO~~) Corrective action has been completed for one of the three recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

20 Dec 2006 ***~~(S//NF)~~ Summary of OIG Oversight 2001-2006 STELLARWIND Program Activities (ST-07-0011)***

~~(S//NF)~~ On 20 December 2006, the OIG issued a report summarizing OIG's oversight of the STELLARWIND Program after five years of implementation.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted] ***~~(TS//SI//NF)~~ Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using Pen Register and Trap and Trace Devices (ST-06-0020)***

~~(TS//SI//NF)~~ On [redacted] the OIG reported that the management controls governing the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the FISC Order authorizing NSA to collect Internet metadata using PR/TT devices were adequate and in several aspects exceeded the terms of the Order. Due to the risk associated with the processing of electronic communications metadata involving U.S. person information, additional controls were needed for processing and monitoring queries made against PR/TT data, documenting

oversight activities, and providing annual refresher training on the terms of the Order.

(U//~~FOUO~~) Corrective action has been completed for two of the six recommendations.

(U//~~FOUO~~) This report was sent to SSCI on [redacted] and HPSCI on [redacted]

5 Jul 2007 ***~~(TS//SI//NF)~~ Domestic Selector Tasking Justification Review (ST-07-0017)***

(U//~~FOUO~~) The OIG conducted this review to determine whether tasking justification statements were supported with intelligence information consistent with sources cited in the justifications. The OIG identified some justifications containing errors, but there was no pattern of errors or exaggeration of facts or intentional misstatements.

(U//~~FOUO~~) This report was sent to SSCI on 28 January 2008 and HPSCI on 28 January 2008.

30 June 2008 ***~~(TS//SI//NF)~~ Advisory Report on the Adequacy of STELLARWIND Decompartmentation Plans (ST-08-0018)***

~~(TS//SI//NF)~~ At the request of the SID Program Manager for CT Special Projects, the OIG assessed the adequacy of NSA's plans to remove data from the STELLARWIND compartment, as authorized by the Director of National Intelligence. On 30 June 2008, the OIG reported that NSA management had a solid foundation of planning for decompartmentation. In particular, the content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of successfully removing data from the STELLARWIND compartment, while complying with laws and authorities. Management was also diligent in assessing the scope and complexity of this undertaking. Although the OIG made no formal recommendations, it suggested improvements to develop more detailed plans, set firm milestones, and establish a feedback system to ensure that plans were successfully implemented.

(U//~~FOUO~~) This report was not sent to SSCI or HPSCI.

APPENDIX F

(U) Presidential Notifications

This page intentionally left blank.

(U) Presidential Notifications

~~(TS//STLW//SI//OC/NF)~~ Executive Orders 12333 and 12863 require intelligence agencies to report to the President, through the President's Intelligence Oversight Board, activities they have reason to believe may be unlawful or contrary to executive order or presidential directive. Knowing that Board members were not cleared, however, the NSA Director or Deputy Director reported the following violations of the Presidential Authorization and related authorities to the President through his Counsel, rather than through the Board. Each notification was approved if not actually drafted by OIG. Some of the notifications were not the subject of the OIG reviews or investigations discussed in Appendix E.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes violations regarding (1) the [redacted] and (2) [redacted]
[redacted]	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes a delay of about 90 days in detasking a telephone number [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes the investigation mentioned above regarding metadata collection violations that occurred under FISA Court Order *In Re* [redacted] FISA Court [redacted] The complete OIG report was issued [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes [redacted] instances in which cleared NSA analysts mistakenly accessed data [redacted] In one instance, a report based on such data went out, but it was not cancelled because the same information was available elsewhere. In the other [redacted] instances, no reports were issued. [redacted]

(U) Date	(U) Summary of Notification
	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes one instance of inadvertent collection of a call with both ends in the U.S. – a fact that could not have been known until it was listened to because [redacted] showed the call as having a foreign origin. [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes three incidents: The first involved a one-digit typo resulting in one incorrectly tasked number. The second involved a number improperly tasked for metadata analysis. The operator discovered it almost immediately and promptly removed it from tasking. The third involved [redacted] numbers that were not detasked in a timely fashion.
2 Aug 2005 [redacted]	~~(TS//SI//NF)~~ Describes the evolving [redacted] a practice that may have resulted in over-collection. The notification refers to NSA's work in developing more rigorous [redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which bulk telephony metadata was actively collected in spite [redacted] At that time NSA limited collection of bulk telephone records to [redacted] as permitted by statute. The collection resulted when [redacted] The error was not discovered for 18 months. ~~(TS//STLW//SI//OC/NF)~~ Although most of the metadata improperly collected was also properly acquired [redacted] pursuant to statute, the dataflow was terminated immediately upon discovery. Also, because the improperly collected metadata had been forwarded to non-STELLARWIND databases, the Agency removed non-compliant metadata from all affected databases, including those in which STELLARWIND data is normally stored.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which an [redacted] This resulted [redacted] of non-target data. The error was discovered within hours, when personnel responsible for monitoring [redacted] The error was corrected, and all inadvertently collected records were deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an instance where a [redacted] Although no reports were generated, and there was no evidence that U.S.-to-U.S. communications were collected, we could not certify that the files were all one-end foreign without reviewing [redacted] The [redacted] files were deleted, and procedures used by [redacted] were being reviewed. ~~(TS//STLW//SI//OC/NF)~~ A second incident was reported in which a typographical error resulted in contact chaining on a U.S. telephone number with no [redacted] affiliation. The telephone number was rechecked, and the error was corrected.

This page intentionally left blank.

APPENDIX G

(U) United States Signals Intelligence Directive SP0018, Legal Compliance and Minimization Procedures

This page intentionally left blank.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES

SIGNALS INTELLIGENCE

DIRECTIVE

18

27 July 1993

INCLUDES CHANGES 1 and 2

See Letter of Promulgation for instructions on reproduction or release of this document.

~~OPC: D2~~
~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

~~SECRET~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES ~~(FOUO)~~

LETTER OF PROMULGATION

(U) This USSID prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18, and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 19.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS, NSTS 963-3121 or [redacted]

J.M.McCONNELL
Vice Admiral, U.S. Navy
Director

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

USSID 18
27 July 1993

CHANGE REGISTER

No	Date	CHANGE Authority (Msg Cite/DTG, Hard Copy (HC))	ENTERED Date	By
1	28OCT97	HARDCOPY CHANGE	29OCT97	RS
2	11Dec98	P0211-0307-98, 111800Z Dec 98	11Dec98	WF
2	11Dec98	P0211-0309-98, 111840Z Dec 98 (correction to above)	11Dec98	WF

This page intentionally left blank.

TABLE OF CONTENTS

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

27 July 1993

USSID 18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES (U)

SECTION 1 – PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

SECTION 2 – REFERENCES

2.1. (U) References

a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.

b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

SECTION 3 – POLICY

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS. The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

SECTION 4 – COLLECTION

4.1. ~~(S-CCO)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] will not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [redacted], or

(c) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(4) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) Technical devices (e.g. [redacted]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted]) and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]:

(a) A non-U.S. PERSON located outside the UNITED STATES [redacted]

(b) [redacted]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process),

sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and abets a person engaging in such activities.

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. ~~(S-CCO)~~ [redacted]

a. [redacted]

b. [redacted]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 3 of this USSID.

4.4. ~~(S-CCO)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that the DIRNSA/CHCSS is advised immediately and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [redacted]

b. If Attorney General approval is obtained, the COLLECTION may continue for the length of time specified in the approval.

c. If it is determined that [redacted] COLLECTION may continue at the discretion of the operational element.

d. If [redacted] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [redacted] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

4.5. ~~(C-CCO)~~ U.S. PERSON TARGETS Entering the UNITED STATES.

a. If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Attorney General approval described in Section 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. ~~(S-CCO)~~ Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [redacted], must be submitted through the DDO and the General Counsel to the DIRNSA/CHCSS for review.

4.7. ~~(C-CCO)~~ Direction Finding. Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for

communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5 – PROCESSING

5.1. ~~(S-CCO)~~ Use of Selection Terms During Processing.
When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located) [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the DDO or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(C-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. ~~(S-CCO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) Establish or maintain intercept, or

(b) Minimize unwanted intercept, or

(c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P02.

5.5. ~~(S-CCO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES [redacted] communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to

warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

SECTION 6 – RETENTION

6.1. ~~(S-CCO)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-CCO)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

SECTION 7 – DISSEMINATION

7.1. ~~(C-CCO)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P02.

7.2. ~~(C-CCO)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made

by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P02 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P02 should be in the form of a CRITICOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

7.3. ~~(C-CCO)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P02, the Deputy Chief, P02, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(1) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P02 within 24 hours of discovery of the error.

SECTION 8 – RESPONSIBILITIES

8.1. (U) Inspector General.
The Inspector General shall:

a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.

b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.

c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.

d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

8.2. (U) General Counsel. The General Counsel shall:

a. Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures should be sent by CRITICOMM to DDI XDI, or by NSA/CSS secure telephone 963-3121, or [redacted]

b. Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.

c. Advise the Inspector General in inspections and oversight of USSS activities.

d. Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, Inspector General or Key Components Chief, all new major requirements and internally generated USSS activities.

e. Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.

f. Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.

g. Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

8.3. (U) Deputy Director for Operations (DDO).
The DDO shall:

a. Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.

b. Apply the provisions of this USSID to all SIGINT production activities. The DDO staff focal point for USSID 18 matters is P02 (use CRITICOMM DDI XAO).

c. Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.

d. Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the General Counsel. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the General Counsel prior to acceptance or execution.

8.4. (U) All Elements of the USSS. All elements of the USSS shall:

a. Implement this directive upon receipt.

b. Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: P02.

c. Immediately inform the DDO of any tasking or instructions that appear to require actions at variance with this USSID.

d. Promptly report to the NSA Inspector General and consult with the NSA General Counsel on all activities that may raise a question of compliance with this USSID.

SECTION 9 – DEFINITIONS

9.1. ~~(S-CCO)~~ AGENT OF A FOREIGN POWER means:

a. Any person, other than a U.S. PERSON, who:

(1) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor; or

(2) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. Any person, including a U.S. PERSON, who:

(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

(2) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation therefor, for or on behalf of a FOREIGN POWER; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in those activities.

c. For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision,

absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

9.2. ~~(S)~~ COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.

9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

b. In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

9.8. ~~(S)~~ FOREIGN COMMUNICATION means a communication that has at least one COMMUNICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

9.10. (U) FOREIGN POWER means:

a. A foreign government or any component thereof, whether or not recognized by the UNITED STATES,

b. A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS,

c. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments,

d. A group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor,

e. A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or

f. An entity that is directed and controlled by a foreign government or governments.

9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. Appear to be intended:

(1) to intimidate or coerce a civilian population,

(2) to influence the policy of a government by intimidation or coercion, or

(3) to affect the conduct of a government by assassination or kidnapping, and

c. Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

9.14. ~~(C)~~ SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [redacted] telephone number, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

9.15. ~~(C)~~ SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the UNITED STATES exercises sovereignty.

9.18. ~~(C)~~ UNITED STATES PERSON:

a. A citizen of the UNITED STATES,

b. An alien lawfully admitted for permanent residence in the UNITED STATES,

c. Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or

d. CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

e. The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(4) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

(5) CORPORATIONS have the nationality of the nation-state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//SI//ORCON/NOFORN~~

No. OP 2008-0009

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

OFFICE OF THE INSPECTOR GENERAL

~~(S//NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

July 2, 2009

ROSLYN A. MAZER
INSPECTOR GENERAL

Copy No.

This page intentionally left blank.

(U) TABLE OF CONTENTS

This page intentionally left blank.

~~(S/NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

I. (U) EXECUTIVE SUMMARY

~~(TS//STLW//SI//OC/NF)~~ The Office of Inspector General (OIG), Office of the Director of National Intelligence (ODNI), was one of five Intelligence Community Inspectors General that conducted a review of their agency's participation in the President's Surveillance Program (hereafter "the Program"), a top secret National Security Agency (NSA) electronic surveillance activity undertaken at the direction of the President. The Program became operational on October 4, 2001, three weeks after the deadly terrorist attacks of September 11, 2001. The review examined the ODNI's involvement in the Program from the period beginning with the stand-up of the ODNI in April 2005 through the termination of the Program in January 2007.

~~(TS//STLW//SI//OC/NF)~~ The ODNI's primary role in the Program was the preparation of the threat assessments that summarized the al Qaeda terrorist threat to the United States and were used to support the periodic reauthorization of the Program. That role began in April 2005, shortly after the ODNI stand-up and contemporaneous with the arrival of General Michael Hayden as the first Principal Deputy Director of National Intelligence (PDDNI). Prior to his ODNI appointment, Hayden was Director of NSA. In April 2005, ODNI personnel in the National Counterterrorism Center (NCTC) began to prepare the first of 12 Program threat assessments. In coordination with the Department of Justice (DOJ), then Director of National Intelligence (DNI) John Negroponte or PDDNI Hayden approved 12 ODNI-prepared threat assessments over an 18-month period. Once approved by the DNI or PDDNI, the Program threat assessments were reviewed and approved by the Secretary of Defense, and were subsequently used by DOJ, NSA, and White House personnel in support of the Program reauthorization. In addition to the preparation of the threat assessments, we found that NCTC used Program information in producing analytical products that were distributed to senior IC community officials and analysts. [redacted]

~~(TS//STLW//SI//OC/NF)~~ During the review, we made several related findings and observations. We learned that the ODNI usage of Program-derived information in ODNI intelligence products was consistent with the standard rules and procedures for handling NSA intelligence. We learned that ODNI personnel were not involved in nominating specific targets for collection through the Program. While ODNI personnel were identified as having contact [redacted] regarding the Program, we found that those communications were limited in frequency and scope. We also found that the ODNI intelligence oversight components -- the Civil Liberties Protection Officer (CLPO), Office of General Counsel (OGC), and the OIG -- had little involvement in oversight of the Program and had limited opportunity to participate in Program oversight due to delays in ODNI oversight personnel being granted access to the

Program and temporary resource limitations attendant to the stand-up of the ODNI. Finally, we found that the 2008 amendments to Executive Order 12333 and the current ODNI staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

II. (U) INTRODUCTION

~~(TS//STLW//SI//OC/NF)~~ *The Foreign Intelligence Surveillance Act Amendments Act of 2008*, Pub L. No. 110-261, 122 Stat. 2438 (hereafter "FISA Amendments Act") required the IGs of the DOJ, ODNI, NSA, Department of Defenses (DOD), and any other element of the intelligence community that participated in the President's Surveillance Program to conduct a comprehensive review of the Program.[1] The FISA Amendments Act defined the "President's Surveillance Program" as the "intelligence activity involving communications authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005." In response to this tasking, the IGs of the following five agencies were identified as having a role in Program review: DOJ, ODNI, NSA, DOD, and the Central Intelligence Agency (CIA).

~~(S//NF)~~ The participating IGs organized the review in a manner where each OIG conducted a review of its own agency's involvement in the Program. CIA IG John Helgerson was initially designated by the IGs to coordinate the review and oversee the preparation of an interim report due within 60 days after the enactment of the Act, and a later final report due not later than 1 year after the enactment of the Act.[2] Because of IG Helgerson's recent retirement, DOJ IG Glenn Fine was selected to coordinate the preparation of the final report. This report contains the results of the ODNI OIG review.

III. (U) SCOPE AND METHODOLOGY

~~(TS//STLW//SI//OC/NF)~~ We sought to identify the role of the ODNI in implementing the Program beginning with the stand-up of the ODNI in April 2005 through the Program's termination in January 2007. This review examined the:

A. Role of the ODNI and its component the National Counterterrorism Center (NCTC) in drafting and coordinating the threat assessments that supported the periodic reauthorization of the Program;

---

[1] ~~(S//NF)~~ The Program is also known within the Intelligence Community by the cover term STELLARWIND. The Program is a Top Secret/Sensitive Compartmented Information (SCI) program.

[2] (U) The participating IGs submitted an interim report, dated September 10, 2008, to the Chairman and Ranking member of the Senate Select Committee on Intelligence (SSCI) and a revised interim report, dated November 24, 2008, to the Chairman and Ranking member of the House of Representatives Permanent Select Committee on Intelligence (HPSCI).

B. NCTC's use of Program information to support counterterrorism analysis;

C. NCTC's role in identifying Program targets and tasking Program collection;

D. [redacted] and

F. Role of the ODNI in providing compliance oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ During the review, we interviewed 23 current or former ODNI officials and employees involved in the Program. The ODNI personnel we interviewed were cooperative and helpful. Our interviews included the following ODNI senior officials:

John Negroponte, former Director of National Intelligence
Michael McConnell, former Director of National Intelligence
Michael V. Hayden, former Principal Deputy Director of National Intelligence
Ronald Burgess, former Acting Principal Deputy Director of National Intelligence
David R. Shedd, Deputy Director of National Intelligence for Policy, Plans, and Requirements
Alexander W. Joel, Civil Liberties Protection Officer
Edward Maguire, former Inspector General
Benjamin Powell, former General Counsel
Corin Stone, Deputy General Counsel and Acting General Counsel
Joel Brenner, former National Counterintelligence Executive[3]
John Scott Redd, former NCTC Director
Michael Leiter, NCTC Director

~~(S//NF)~~ In addition to the interviews noted above, we reviewed Program-related documents made available by the NSA OIG, the DOJ OIG, and the ODNI OGC.

IV. (U) DISCUSSION OF FINDINGS

~~(TS//STLW//SI//OC/NF)~~ The following discussion contains our findings regarding the topics identified above. First, we briefly describe the terrorist attacks of September 11, 2001, and the initial government response to the attacks, including the authorization of the President's Surveillance Program. Next, we discuss the ODNI and NCTC role in implementing the Program. Finally, we set forth our conclusions and observations.

A. (U) Initial Response by the President and Congress to the Terrorist Attacks of September 11, 2001

(U) The devastating al Qaeda terrorist attacks against the United States quickly triggered an unprecedented military and intelligence community response to protect the

[3] (U) Brenner was the NSA Inspector General before joining the ODNI.

country from additional attacks. The following quote describes the initial terrorist attacks and the intended al Qaeda goal to deliver a decapitating strike against our political institutions.

> (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial airliners, each carefully selected to be fully loaded with jet fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States – to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths – the highest single-day death toll from hostile foreign attacks in the Nation's history.[4]

(U) On September 14, 2001, in response to the attacks, the President issued a *Declaration of National Emergency by Reason of Certain Terrorist Attacks* stating that "(a) national emergency exists by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and continuing immediate threat of further attacks on the United States."[5]

(U) On September 18, 2001, by an overwhelming majority in both the Senate and House of Representatives, a joint resolution was passed that authorized the use of United States military force against those responsible for the terrorist attacks launched against the United States. The joint resolution, also known as the *Authorization for Use of Military Force (AUMF)*, is often cited by White House and DOJ officials as one of the principal legal authorities upon which the Program is based. In relevant part, the AUMF provides:[6]

> (a) IN GENERAL – That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organization or persons, in order to

[4] (U) This summary of the events of September 11, 2001, was prepared by DOJ personnel and is set forth in the unclassified DOJ "White Paper" entitled *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, dated January 19, 2006.

[5] (U) Proclamation 7463, 66 Fed. Reg. No. 181, September 14, 2001.

[6] (U) *Authorization for Use of Military Force*, Section 2(a), Pub. L. No. 170-40, 115 Stat. 224, September 18, 2001.

prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

~~(TS//STLW//SI//OC/NF)~~ On October 4, 2001, three days before the start of overt military action against the al Qaeda and Taliban terrorist camps, the President authorized the Secretary of Defense to implement the President's Surveillance Program.[7] The Program, a closely held top-secret NSA electronic surveillance project, authorized the Secretary of Defense to employ within the United States the capabilities of the DOD, including but not limited to the signals intelligence capabilities of the NSA, to collect international terrorism-related foreign intelligence information under certain specified circumstances. Each Program reauthorization was supported by a written threat assessment, approved by a senior Intelligence Community official, that described the threat of a terrorist attack against the United States.

(U) On October 7, 2001, in a national television broadcast, the President announced the start of military operations against al Qaeda and Taliban terrorist camps in Afghanistan.[8]

~~(TS//STLW//SI//OC/NF)~~ On April 22, 2005, the ODNI began operations as the newest member of the Intelligence Community. The ODNI was created, in part, in response to the findings of the *Independent National Commission on Terrorist Attacks Upon the United States* (hereafter 9/11 Commission) that recommended the creation of a national "Director of National Intelligence" to oversee and coordinate the planning, policy, and budgets of the Intelligence Community.[9] In late April 2005, ODNI personnel began to prepare the threat assessments used in the periodic reauthorization of the Program. In June 2005, ODNI officials began to approve the threat assessments.

B. ~~(TS//STLW//SI//OC/NF)~~ ODNI Role in Preparing Threat Assessments in Support of the Program Reauthorizations

~~(TS//STLW//SI//OC/NF)~~ Prior to the ODNI's involvement in the Program, the Program was periodically reauthorized approximately every 30 to 45 days pursuant to a reauthorization process overseen by DOJ, NSA, and White House personnel. Each reauthorization relied, in part, on a written threat assessment approved by a senior Intelligence Community official that described the current threat of a terrorist attack against the United States and contained the approving official's recommendation regarding the need to reauthorize the Program. Before the ODNI's involvement in the

---

[7] ~~(TS//STLW//SI//OC/NF)~~ The NSA materials we reviewed identified October 4, 2001, as the date of the first Program authorization.

[8] (U) The CNN.com webpage article entitled *President announces opening of attack*, dated, October 7, 2001, provides a summary of the President's announcement and describes the national television broadcast.

[9] (U) While the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) that created the ODNI was signed by the President on December 17, 2004, the actual ODNI stand-up occurred months later. The official ODNI history, *A Brief History of the ODNI's Founding*, sets April 22, 2005, as the date when the ODNI commenced operations.

Program, every threat assessment prepared by the Intelligence Community in support of the Program reauthorization identified the threat of a terrorist attack against the United States and recommended that the Program be reauthorized. Accordingly, the Program was regularly reauthorized during the approximately 3-year period prior to the involvement of the ODNI. During that period, the Director of Central Intelligence or his designee approved 31 threat assessments in support of the reauthorization of the Program.

~~(TS//STLW//SI//OC/NF)~~ In reviewing the circumstances that led to the decision to transfer responsibility for preparing the Program threat assessments to the ODNI, we found that the ODNI does not have identifiable records regarding that decision. Senior ODNI officials involved with the Program told us that after the merger of the Terrorist Threat Integration Center (TTIC) into the NCTC, and the later incorporation of NCTC into the ODNI, it made sense for the ODNI to take responsibility for preparing the Program threat assessments as both TTIC and NCTC previously handled that task. Former PDDNI Hayden told us that the primary reason that the ODNI become involved in the Program was the statutory creation of the new DNI position as the senior Intelligence Community advisor to the President. When Ambassador Negroponte was confirmed as the first DNI, Hayden and other senior intelligence officials believed that DNI Negroponte, as the President's new senior intelligence advisor, should make the Intelligence Community's recommendation to the President regarding the need to renew the Program. Hayden commented that the new DNI's involvement in this important intelligence program enhanced the DNI's role as the leader of the Intelligence Community and gave immediate credibility to the ODNI as a new intelligence agency.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI became involved in the Program, the preparation and approval of the threat assessments became the ODNI's primary Program role.[10] Beginning in April 2005, and continuing at about 30 to 45 day intervals until the Program's termination in January 2007, ODNI personnel prepared and approved 12 written threat assessments in support of the periodic reauthorization of the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel who prepared the documents following an established DOJ format used in earlier Program reauthorizations. NCTC analysts prepared the threat assessments in a memorandum format, usually 12 to 14 pages in length. Senior ODNI and NCTC officials told us that each threat assessment was intended to set forth the ODNI's view regarding the current threat of an al Qaeda attack against the United States and to provide the DNI's recommendation whether to continue the Program. NCTC personnel involved in preparing the threat assessments told us that the danger of a terrorist attack described in the threat assessments was sobering and "scary," resulting in the threat assessments becoming known by ODNI and Intelligence Community personnel involved in the Program as the "scary memos."

[10] ~~(TS//STLW//SI//OC/NF)~~ The joint interim report prepared by the participating IGs notified congressional oversight committees that the review would examine the ODNI's involvement in preparing "threat assessments and legal certifications" submitted in support of the Program. Because we did not identify any ODNI officials executing a legal certification, we treated our review of the legal certifications to be the same as the review of the threat assessments. The Attorney General made legal certifications in support of the Program that are addressed in the DOJ OIG report.

~~(TS//STLW//SI//OC/NF)~~ During interviews, ODNI personnel said they were aware that the threat assessments were relied upon by DOJ and the White House as the basis for continuing the Program and further understood that if a threat assessment identified a threat against the United States, the Program was likely to be reauthorized. NCTC analysts also said that on a less frequent basis they prepared a related document that set forth a list of al Qaeda-affiliated groups that they understood were targets of the Program. Both the threat assessments and the less frequent list of al Qaeda-affiliated groups underwent the same ODNI approval process.

~~(TS//STLW//SI//OC/NF)~~ We examined the ODNI process for preparing the Program documents, particularly the threat assessments, and found that the documents were drafted by experienced NCTC analysts under the supervision of the NCTC Director and his management staff, who were ultimately responsible for the accuracy of the information in the documents. We determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide-variety of Intelligence Community sources. ODNI personnel told us that during the period when the ODNI prepared the threat assessments, the Intelligence Community had access to fully evaluated intelligence that readily supported the ODNI assessments that al Qaeda terrorists remained a significant threat to the United States.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI threat assessments were approved within NCTC and by the NCTC Director, the documents were forwarded through an established approval chain to senior ODNI personnel who independently satisfied themselves that the documents were accurate, properly prepared, and in the appropriate format. Throughout the ODNI preparation and approval process, the threat assessments were also subject to varying degrees of review and comment by DOJ and OGC attorneys, including then General Counsel Benjamin Powell and Deputy General Counsel Corin Stone. Powell said his review of the threat assessments was not a legal review, but was focused on spotting issues that might merit further review or analysis. Powell said he relied on DOJ to conduct the legal review. Once the draft threat assessments were subjected to this systematic and multi-layered management and legal review, the documents were provided to the DNI or PDDNI for consideration and, if appropriate, approval. Overall, we found the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI or PDDNI approval.

~~(TS//STLW//SI//OC/NF)~~ Negroponte told us that because of time-sensitive issues present in 2005 relating to the ongoing ODNI start-up as a new agency and other Intelligence Community matters requiring his attention, he tasked his deputy, then PDDNI Hayden, to oversee the ODNI approval of the threat assessments and related documents. Negroponte told us that when making this decision, he was aware of Hayden's prior experience with the Program during Hayden's earlier assignment as Director of NSA. In June 2005, shortly after his arrival at ODNI, Hayden received and approved the first ODNI threat assessment. Hayden later approved the next six ODNI threat assessments. After Hayden left the ODNI in May 2006 to become Director of CIA, Negroponte approved the next five ODNI threat assessments, including a December

2006 threat assessment used in the final reauthorization of the Program. In total, Negroponte and Hayden approved 12 ODNI threat assessments prepared in support of the Program reauthorizations.[11]

~~(TS//STLW//SI//OC/NF)~~ In discussing the ODNI process used to prepare and approve the threat assessments, Negroponte told us he was "extremely satisfied" with the quality and content of the threat assessments provided for his approval. He did not recall any inaccuracies or problems relating to preparation of the ODNI threat assessments. Negroponte said the al Qaeda threat information described in the Program threat assessments was consistent with the terrorism threat information found in *The President's Daily Briefing* and other senior-level Intelligence Community products he had read. Hayden had a similar view. Negroponte and Hayden separately told us that when they approved the threat assessments, credible intelligence was readily available to the Intelligence Community that demonstrated the ongoing and dangerous al Qaeda terrorist threat to the United States. Similarly, Negroponte and Hayden each told us that the nature and scope of the al Qaeda terrorist threat to the United States was well documented and easily supported the ODNI threat assessments used in the Program reauthorizations.

~~(TS//STLW//SI//OC/NF)~~ Because of questions raised in the media about the legal basis for the Program, we asked the ODNI personnel involved in the preparation or approval of the threat assessments about their concerns, if any, regarding the legal basis for the Program. We found that ODNI personnel involved in the Program generally understood that the Program had been in operation for several years and was approved by senior Intelligence Community and DOJ officials. During our interviews, ODNI officials told us they were satisfied with the legal basis for the Program, primarily because of their knowledge that the Attorney General and senior DOJ attorneys had personally approved the Program and remained directly involved in the Program reauthorization process. We did not identify any ODNI personnel who believed that the program was unlawful.

~~(TS//STLW//SI//OC/NF)~~ Former ODNI General Counsel Powell told us that after his Program briefings in early 2006, he had questions regarding the DOJ description of the legal authority for the Program but lacked the time to conduct his own legal review of the issue given the many time-sensitive ODNI legal issues that required his attention. Powell said he understood the rationale of DOJ's legal opinion that the Program was lawful and described the DOJ opinion as a "deeply complex issue" with "legal scholarship on both sides." Powell said he recognized that he was a latecomer to a complex legal issue that was previously and continuously approved by DOJ, personally supported by the Attorney General, and was being transitioned to judicial oversight – an idea he strongly supported. Powell said he relied on the DOJ legal opinion regarding the Program and directed his efforts to supporting the Program's transition to judicial oversight under traditional FISA, the 2007 Protect America Act, and the subsequent FISA Amendments Act of 2008.

---

[11] ~~(TS//STLW//SI//OC/NF)~~ The DNI and PDDNI together approved 12 of the 43 threat assessments used in support of the Program reauthorizations. CIA officials approved the other 31 threat assessments.

~~(TS//STLW//SI//OC/NF)~~ Negroponte recalled having regular contact with senior NSA and DOJ officials who raised no legal concerns to him about the Program. He said he remembered attending a Program-related meeting that included members of the FISA Court who did not raise any legal concerns to him about the authority for the Program and seemed generally supportive of the Program. Negroponte also recalled attending meetings in which the Program was briefed to congressional leadership who not did raise legal concerns to him. Overall, the direct involvement of DOJ and other senior Intelligence Community officials in the Program resulted in Negroponte and other ODNI personnel having few, if any, concerns about the legal basis for the Program.

C. ~~(TS//STLW//SI//OC/NF)~~ NCTC Use of Program Information to Support Counterterrorism Analysis

~~(TS//STLW//SI//OC/NF)~~ The Program information was closely held within the ODNI and was made available to no more than 15 NCTC analysts for review and, if appropriate, use in preparing NCTC analytical products.[12] Generally, the NCTC analysts approved for access received the Program information in the form of finished NSA intelligence products. [redacted] The NCTC analysts said the Program information was subject to stringent security protections [redacted] The NCTC analysts told us they received training regarding proper handling of NSA intelligence. They said they handled the NSA intelligence, including Program information, consistent with the standard rules and procedures for handling NSA intelligence information, including the minimization of U.S. person identities.

~~(TS//STLW//SI//OC/NF)~~ Hayden told us that during his tenure as Director of NSA, he sought to disseminate as much Program information as possible to the Intelligence Community [redacted]

~~(TS//STLW//SI//OC/NF)~~ During our review, NCTC analysts told us they often did not know if the NSA intelligence available to them was derived from the Program. [redacted]

[12] ~~(TS//STLW//SI//OC/NF)~~ The number of NCTC analysts read into the Program ranged from 5 to 15 analysts.

[redacted] On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the Program, the analysts said they reviewed the Program information in the same manner as other NSA intelligence products and, if appropriate, incorporated the Program information into analytical products being prepared for the DNI and other senior intelligence officials. They identified the *President's Terrorism Threat Report* and the *Senior Executive Terrorism Report* as examples of the types of finished intelligence products that would, at times, contain Program information.

~~(TS//STLW//SI//OC/NF)~~ NCTC analysts with Program access said they had broad access to a wide variety of high quality and fully evaluated terrorism related intelligence. In particular, NCTC analysts told us that by virtue of their NCTC assignments, they had access to some of the most sensitive and valuable terrorism intelligence available to the Intelligence Community. NCTC analysts characterized the Program information as being a useful tool, but also noted that the Program information was only one of several valuable sources of information available to them from numerous collection sources and methods. During interviews, NCTC analysts and other ODNI personnel described the Program information as "one tool in the tool box," "one arrow in the quiver," or in other similar phrases to connote that the Program information was not of greater value than other sources of intelligence. The NCTC analysts we interviewed said they could not identify specific examples where the Program information provided what they considered time-sensitive or actionable intelligence, but they generally recalled attending meetings in which the benefits of the Program were discussed. [redacted] The NCTC analysts uniformly told us that during the period when NCTC prepared the threat assessment memoranda, the intelligence demonstrating the al Qaeda threat to the United States was overwhelming and readily available to the Intelligence Community.

~~(TS//STLW//SI//OC/NF)~~ When asked about the value of the Program, Hayden said "without the Program as a skirmish line you wouldn't know what you don't know." He explained that by using the Program to look at a "quadrant of communications" the Intelligence Community was able to assess the threat arising from those communications, which allowed Intelligence Community leaders to make valuable judgments regarding the allocation of national security resources. He said looking at the terrorist threat in this manner was similar to soldiers on a combat patrol who look in all directions for the threat and assign resources based on what they learn. Hayden said that NSA General Counsel Vito Potenza often described the Program as an "early warning system" for terrorist threats, which Hayden thought was an accurate description of the Program. Hayden told us the Program was extremely valuable in protecting the United States from an al Qaeda terrorist attack. Hayden cited [redacted].

[redacted] as examples where the Program information was effectively used to disrupt al Qaeda operatives.[13]

D. [redacted]

[redacted]

13 [redacted]

[redacted]

E. ~~(TS//STLW//SI//OC/NF)~~ No NCTC Role in Identifying Program Targets and Tasking Collection

~~(TS//STLW//SI//OC/NF)~~ We did not identify any information that indicated that ODNI or NCTC personnel were involved in identifying or nominating targets for collection within the Program. ODNI personnel told us that ODNI and NCTC are non-operational elements of the Intelligence Community and were not involved in nominating targets for Program collection.

F. ~~(S/NF)~~ ODNI Oversight of the Program

~~(TS//STLW//SI//OC/NF)~~ We examined the role of the ODNI oversight components -- CLPO, OIG, and OGC -- in providing compliance oversight for the Program. We found that while the Program was subject to oversight by the NSA OIG, the ODNI oversight components had a limited role in providing oversight for the Program. During the review, we learned that within the first year of the Program, then NSA Director Hayden obtained White House approval allowing the NSA IG and designated NSA OIG officials to be read into the Program to provide compliance oversight for the Program. In furtherance of the NSA oversight program, the NSA IG provided compliance reports and briefings to the NSA Director, NSA General Counsel, and cleared White House personnel, including the Counsel to the President.[16]

~~(TS//STLW//SI//OC/NF)~~ In reviewing the ODNI oversight role regarding the Program, we found that the ODNI oversight components had limited involvement in oversight of the Program. We found that the opportunity for the ODNI to participate in Program oversight was limited by the fact that ODNI oversight personnel were not

[redacted]

[15] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[16] ~~(S//NF)~~ According to the General Counsel to the President's Intelligence Oversight Board (IOB), the IOB members and staff were not read into the Program and did not receive compliance reports from the NSA IG.

granted timely access to the Program by the White House personnel responsible for approving access. In addition, we found that the newly formed ODNI oversight offices were in varying stages of agency stand-up and lacked the necessary experienced staff and resources to effectively participate in oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ For example, General Counsel Powell received Program access after his arrival in January 2006, but his predecessor, then Acting General Counsel Corin Stone, was not read into the Program until a few days before Powell in January 2006, several months after the Program became operational within ODNI and only after she had read about the Program in a December 2005 newspaper article.[17] Similarly, CLPO Alexander Joel, who is responsible for reviewing the privacy and civil liberties implications of intelligence activities, requested but did not receive Program access until October 2006, shortly before the Program terminated.[18] Joel told us that Negroponte and Hayden supported his request for Program access, but White House staff delayed approval for several months. Joel said that while waiting for approval of his Program access, Hayden gave him some insight about the Program that did not require the disclosure of compartmented information. Joel found this information helpful in planning his later review. Finally, then ODNI Inspector General Edward Maguire and his oversight staff did not obtain Program access until 2008, long after the Program had terminated.[19]

~~(TS//STLW//SI//OC/NF)~~ Once read into the Program, Powell and Joel were provided with reasonable access to NSA compliance reports and briefings relating to the NSA OIG oversight program. Powell told us that he was satisfied that the NSA IG provided a reasonable degree of Program oversight. Similarly, Joel said he believed that he had received full disclosure regarding the NSA oversight program and found the NSA oversight effort to be reasonable.

~~(TS//STLW//SI//OC/NF)~~ We also learned that the members of the President's Privacy and Civil Liberties Oversight Board (PCLOB) reviewed the Program, in part, in association with Joel.[20] The PCLOB review was contemporaneous with Joel's review

---

[17] (U//~~FOUO~~) Powell was appointed General Counsel in January 2006 and served in that position as a recess appointment until his Senate confirmation in April 2006. Prior to his appointment, Powell was an Associate Counsel to the President and Special Assistant to the President where he worked on initiatives related to the Intelligence Community. However, Powell was not read into the Program while serving at the White House.

[18] (U//~~FOUO~~) Joel is the Civil Liberties Protection Officer (CLPO) with the responsibility for ensuring that the protection of privacy and civil liberties is incorporated in the policies and procedures of the Intelligence Community. The CLPO responsibilities are set forth in the Section 103d of *Intelligence Reform and Terrorism Prevention Act of 2004.*

[19] ~~(S//NF)~~ While OIG personnel were not read into the Program until 2008, OIG officials were alerted to the existence of the NSA collection program through a December 2005 newspaper report. Shortly after that report, the NSA IG told ODNI OIG officials that the NSA OIG was conducting oversight of that NSA program. PDDNI Hayden also told IG Maguire that the NSA program was subject to NSA OIG oversight.

[20] (U) The PCLOB was created by the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, which requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism (P.L. 108-458, 2004).

and resulted in an independent and generally favorable finding regarding the NSA implementation of the Program. After the PCLOB review, a PCLOB board member published an editorial article, in part, quoted below, that summarized his observations regarding the NSA effort in implementing the Program.

> There were times, including when the Board was "read into" and given complete access to the operation of the Terrorist Surveillance Program that I wondered whether the individuals doing this difficult job on behalf of all of us were not being too careful, too concerned, about going over the privacy and liberties lines – so concerned, with so many internal checks and balances, that they could miss catching or preventing the bad guys from another attack. And I remember walking out of these briefing sessions in some dark and super-secret agency with the thought: I wish the American people could meet these people and observe what they are doing.[21]

~~(S//NF)~~ In sum, the ODNI oversight components had limited and belated involvement in the oversight of the Program. However, once read into the Program, Powell and Joel determined that the Program was subject to reasonable oversight by the NSA OIG. Moreover, the initial White House delay in granting ODNI oversight personnel access to the Program occurred prior to the 2008 revision to Executive Order (EO) 12333, which expressly grants ODNI oversight components broad access to any information necessary to performing their oversight duties. In particular, EO 12333 provides in relevant part that:

> Section 1.6 *Heads of Elements of the Intelligence Community*. The heads of elements of the Intelligence Community shall:
>
> (h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy and civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their duties.

~~(TS//STLW//SI//OC/NF)~~ EO 12333, as amended, clarifies and strengthens the ODNI's ability to provide compliance oversight. In light of the recent change to EO 12333, and with current staffing, we believe that ODNI's oversight components have sufficient resources and authority to perform their responsibilities to conduct oversight of closely held intelligence activities, assuming timely notification.

---

[21] (U) The quote is taken from a May 5, 2007, article by former PCLOB member Lanny Davis, entitled, "*Why I Resigned From The President's Privacy and Civil Liberties Oversight Board – And Where We Go From Here.*" The article was published on webpage of The Huffington Post, www.huffingtonpost.com.

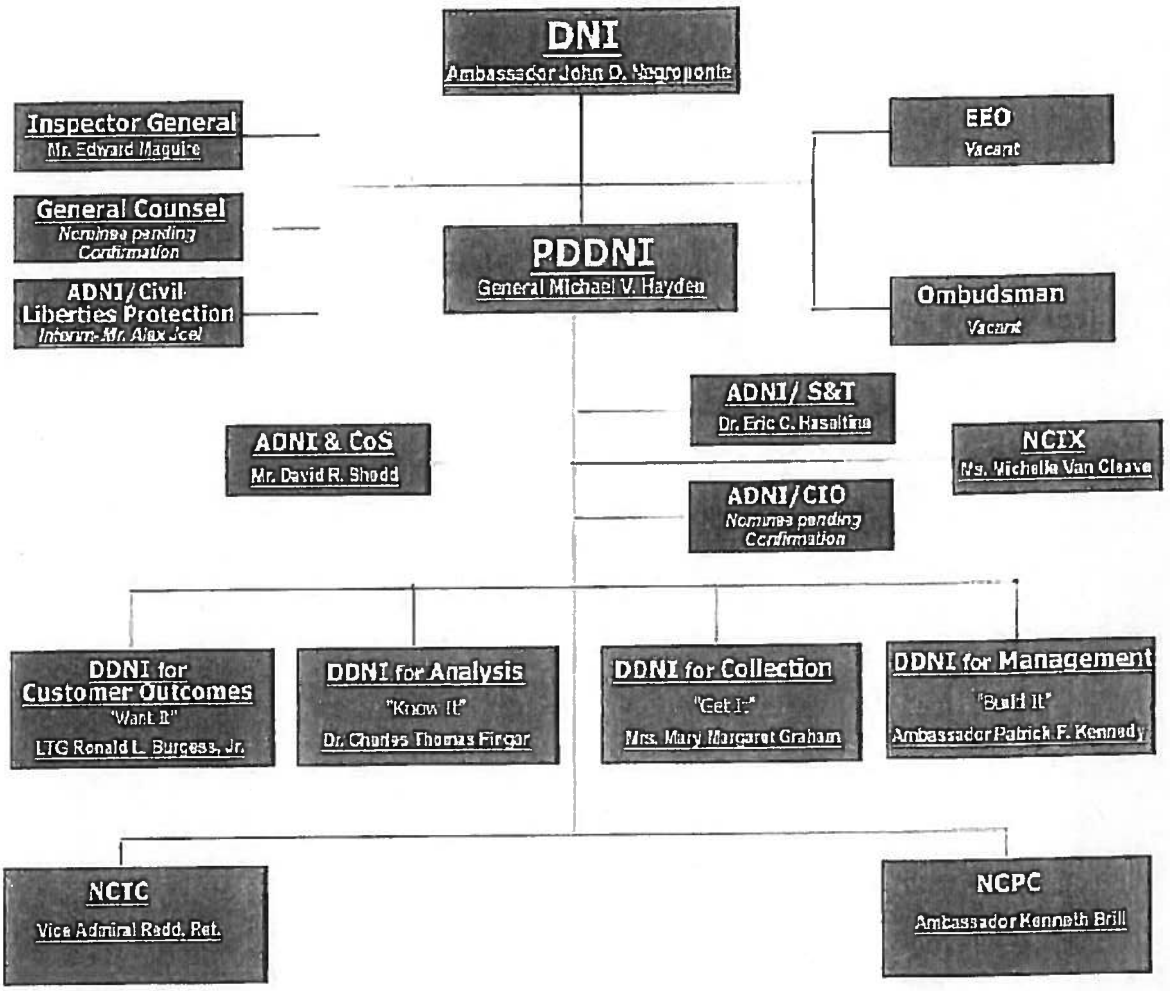
V. (U) CONCLUSION

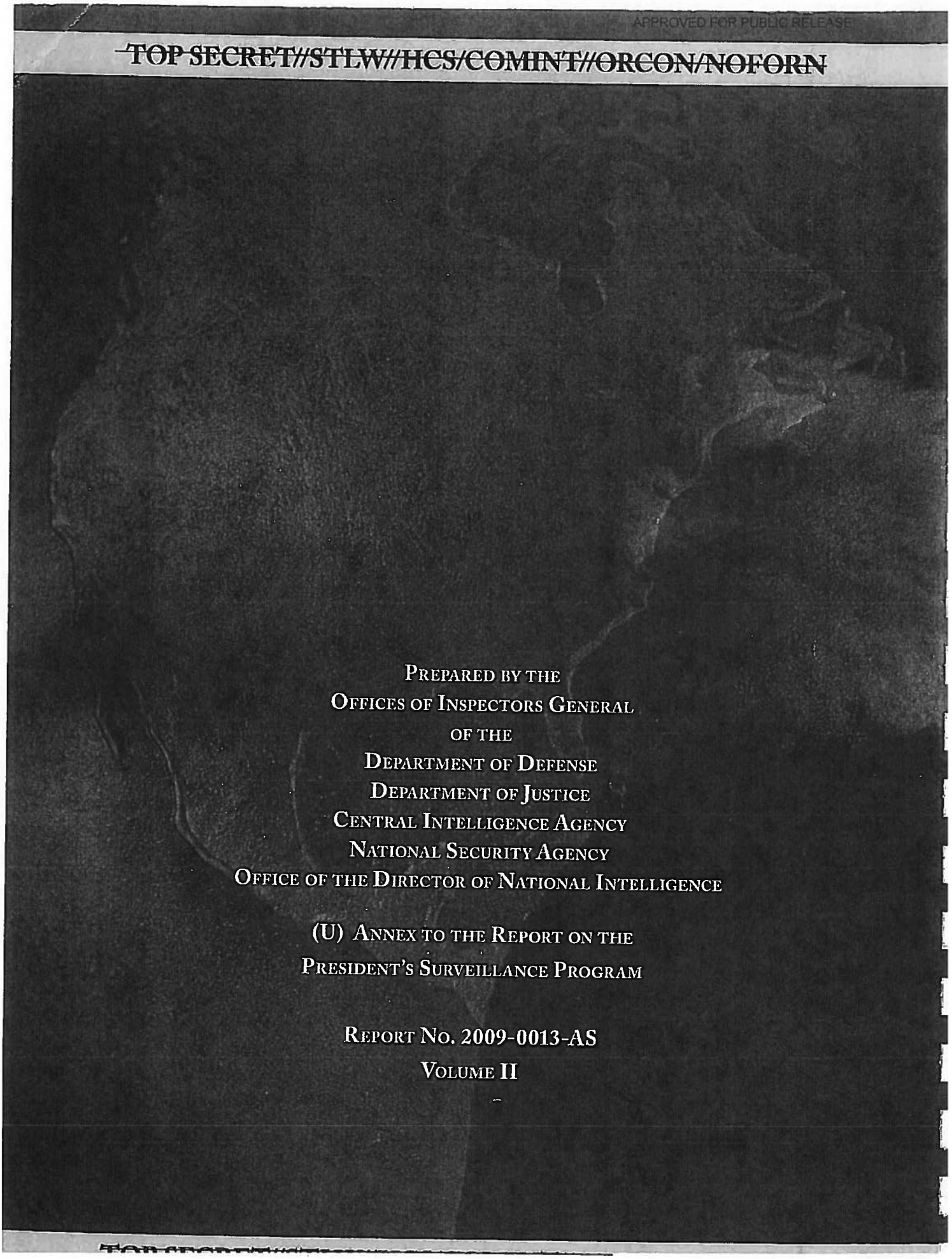
~~(TS//STLW//SI//OC/NF)~~ We found that the ODNI's primary role in the Program was the preparation of 12 ODNI threat assessments approved by the DNI or PDDNI for use in the Program reauthorizations. The ODNI-prepared threat assessments set forth the ODNI's view regarding the existing threat of an al Qaeda terrorist attack against the United States and provided the DNI's recommendation regarding the need to reauthorize the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel under the supervision of knowledgeable NCTC supervisors. We noted that the threat assessments were subject to review by OGC and DOJ attorneys before approval. Additionally, we found that the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI approval. Overall, we found the ODNI process for the preparation and approval of the threat assessments was responsible and effective.

~~(TS//STLW//SI//OC/NF)~~ We also found that the ODNI oversight components played a limited role in oversight of the Program. The limited ODNI oversight role was due to delays in obtaining Program access for ODNI oversight personnel and to temporary resource limitations related to the stand-up of the agency. However, we believe that the 2008 amendments to EO 12333 and improved staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

This page intentionally left blank.

VI. (U) APPENDIX - STRUCTURE OF THE ODNI – 2005





PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS
VOLUME II